SesameStreet++

James Rowell

February 10, 2017

There are 10 sorts of people in the world: those who understand binary and those who don't.

Most of us think about "whole numbers" not too differently from the way we learned to count by watching Sesame Street, the difference being that now we can count a little higher. How we've trained ourselves, it's automatic to think the way that we write a number or say a number *is* the number.

If I owe you 13 cents and I give you one dime and three pennies then after thanking me profusely for repaying this staggering debt, we'll agree that it's settled with those coins equaling 13 pennies. We identify the symbol "13" very strongly with this particular number - it would be tough to get through life in the modern world without such an automatic process running in our brains. This example highlights what this particular symbol "13" actually means - one dime (1×10) plus three pennies (3×1).

Let's look at the number 13 in some alternative ways - it's the number of months in a year plus one month; what I'm suggesting is that there is no need for the symbol "13" in order to think about this particular number of months. Similarly, 13 is this many apples ; or 13 is the sixth prime number. None of these ways of thinking about the number 13 require that we represent it using the digits 1 and 3 butted up next to each other.

Each number exists independently from any symbol or word that might represent it. Numbers are an idea - perhaps such a strong idea that the universe wouldn't exist without them! Anyway, for our purposes whole numbers exist in some abstract realm - Each number is one whole unit more than the previous number, starting at nothing, that is "zero", and jumping to something, that is "one", then one more, which gets us to "two", then again to "three", etc. Continuing in this way forever... we get them all.

To get back to the idea of what a whole number really is, try to forget about the symbols or words we use and picture a pile of apples. There are zero apples (it's hard to show no-apples), then we introduce an "" to get our very first, and smallest, non-empty pile of apples. Then add another apple to get a pile of "", then "", then "" then some big pile of "..." after we've been adding apples for a while. Each successively bigger pile of apples corresponds with each successive whole number. We expand this entire set of whole numbers to include their negative-counterparts and call this larger set "integers".

However, using a "1" followed by a "3" to represent the integer "" is VERY handy. So we use Hindu-Arabic numbers and the positional notation of "base-ten", more commonly known as "decimal", to represent each specific integer. We slap a "-" on the front if we need to talk about a negative integer.

Base-ten representation of an integer is far superior to ancient Roman numerals for example. Try adding two numbers together in ancient Rome, or worse, multiplying or dividing them. What's XI times IX? Would you believe me if I told you it's XCIX? Unless you convert those to Hindu-Arabic numerals to check, you're just gonna have to trust me. Truth is - I don't know how to multiply using Roman numerals - nor did most Romans! Not only that, but I'll bet that most kids who graduated from Sesame Street can count higher than any Roman could - as the Roman system only effectively allowed counting up to 4999.

Using base-ten for us is automatic, we barely think about it when we're adding numbers or multiplying them - but it's worth looking carefully at how base-ten works - so let's examine it from the ground up*.

It's useful to have simple symbols to represent each of the integers from one to nine, namely our familiar 1, 2, 3, 4, 5, 6, 7, 8 and 9 which have an interesting history and predate their use in base-ten.

Slightly more modern, but still quite ancient, is the symbol "0" for "zero", originally meaning "empty". Zero also predates its use in base-ten but without zero, base-ten wouldn't be possible.

Base-ten uses the idea of stringing a series of digits together (a digit being one of the numbers 0, 1, 2, ... 9), one after the other to be able to represent each whole number. Let's look at the first two-digit number, that is, ten, which as you well know looks like this: "10". This extra digit on the left tells us how many tens we have and the last, or rightmost digit says how many additional units to add to it.

So our very first two-digit number 10 means "one lot of ten - plus zero units". When we see "11" - we interpret it to mean "one lot of ten - plus one unit", and "12" is "one lot of ten - plus two units", etc.

Continuing on; "20" - we interpret to mean "two lots of ten, plus zero units", etc. up to "90" meaning "nine lots of ten, plus zero units".

Following this line of reasoning since "10" now means the integer ten, then "100" must mean "ten lots of ten, plus zero units"- which is exactly what it means. We have a special word for this number we call it "one hundred" or "one lot of a hundred, plus zero lots of tens, plus zero units". Similarly "200" means "two lots of a hundred, plus zero lots of ten, plus zero units", etc.

We can keep going by one-hundred until we similarly get to "1000" or "ten lots of a hundred, plus zero lots of ten, plus zero units" otherwise known as "a thousand" or more specifically "one lot of a thousand, plus zero lots of a hundred, plus zero lots of ten, plus zero units".

It gets a little tedious to be so specific when reading out a number so our language has developed quite a few verbal shortcuts. Furthermore it doesn't take long before we run out of fancy names for these "powers-of-ten" like, million, billion, trillion, zillion etc. So let's introduce some nice clean mathematical notation to describe these powers-of-ten and let's forget the fancy words.

---

*Please forgive the incredibly obvious nature of much of the following discussion, but I want to take a good running start at some more unfamiliar notions. Perhaps looking at the familiar with fresh eyes will help in seeing the new ideas easier.

$$100 = 10 \times 10 = 10^2,$$
$$1000 = 10 \times 10 \times 10 = 10^3,$$
$$10000 = 10 \times 10 \times 10 \times 10 = 10^4,$$
$$\ldots$$
$$\underbrace{10\ldots000}_{k \text{ zeros}} = \underbrace{10 \times 10 \times 10 \times 10 \times \ldots \times 10}_{k \text{ 10s}} = 10^k$$

10^k means there are k tens multiplied together - also written as a 1 followed by k zeros[*]. The above list explicitly shows the cases for $k = 2, 3$ and 4. Using the k like that is just a way to show that we can pick ANY whole number, i.e., there is no limit on how big k can be.

The notation of 10^k is very handy, in fact it extends to the case when $k = 0$ and $k = 1$.

So 10^1 means[†] that there is only one ten multiplied together, or one "0" following the "1", in other words just the number ten itself.

How about when $k = 0$? Examining the pattern of how the power k relates to how many zeros follow the "1" (eg, $10^1 = 10$, $10^2 = 100$, $10^3 = 1000$, etc.) then it must be the case that $10^0 = 1$, i.e., no zeros follow the "1", which is exactly right. Furthermore every number raised to the 0th power is 1.[‡]

Let's look at an example. Reading the number 92507 out according to our technique we can see that it's "nine lots of ten-thousand, plus two lots of a thousand, plus five lots of a hundred, plus zero lots of ten, plus seven units":

	9	×	10000			90000
+	2	×	1000		+	2000
+	5	×	100	=	+	500
+	0	×	10		+	00
+	7	×	1		+	7
					=	92507

Written[§] in terms of powers-of-ten: $92507 = 9\times10^4 + 2\times10^3 + 5\times10^2 + 0\times10^1 + 7\times10^0$.

This way of breaking down the base-ten representation of a number into an algebraic expression can be done for EVERY string of decimal digits. It's the key to understanding what a string of decimal digits means.

Recalling that $10^0 = 1$ you might wonder why we bother to multiply $7\times10^0 = 7\times1 = 7$ since there is no actual effect when multiplying by one. Even though it's not necessary, including the 10^0 in the expression reveals a kind of mathematical symmetry. Each successive digit is multiplied by an ever decreasing power-of-ten, including the units digit, which is just some number from 0 to 9 times a power-of-ten like any of the other digits.

---

[*]k is called the "exponent" and you should read the symbol 10^k as "ten-raised-to-the-k^{th}-power" or "ten-to-the-k", so 10^2 is "ten raised to the second power" or 10^4 is "ten-to-the-fourth". You may also see 10^2 referred to as "ten squared", similarly 10^3 as "ten cubed" - but since we don't live in 4 dimensional hyperspace, we don't have a way of saying 10^4 that has geometric meaning.

[†]Don't forget to read 10^1 as "ten-to-the-one".

[‡]Proof: Since $a^{b+c} = a^b a^c$ consider when $c = 0$; that is, $a^b = a^{b+0} = a^b a^0$ so because of the uniqueness of the multiplicative identity "1", then a^0 *must* be 1 since it's behaving like a "1" in the expression $a^b = a^b a^0$.

[§]Recall the mnemonic "bedmas" for the "Order of Operations" in evaluating an expression, which is no different from what we did in our table above the expression.

Our example number 92507 only has five digits and it's biggest power-of-ten is 10^4, but there's no limit on how big a power-of-ten could be involved in our expression. Look at "a trillion and one", i.e.; 1,000,000,000,001 which can be expressed as:

$$1 \times 10^{12} + 0 \times 10^{11} + 0 \times 10^{10} + \cdots + 0 \times 10^2 + 0 \times 10^1 + 1 \times 10^0$$

Or pushing that limit to silly heights we can also describe this next ludicrous number. It's twenty-thousand-and-one digits long, a "7" followed by 9999 zeros, then a "3" followed by 9999 more zeros, then a "5", which means this:

$$7 \times 10^{20000} + 0 \times 10^{19999} + \cdots + 0 \times 10^{10001} + 3 \times 10^{10000} + 0 \times 10^{9999} + \cdots + 0 \times 10^1 + 5 \times 10^0$$

Clearly we can keep going as high as we like.

But how do we *know* that we can create ALL the positive integers with this scheme? How do we *know* that we didn't miss one? How do we *know* that some string of digits doesn't represent two different integers? I know it seems silly to ask these kinds of questions - after all, people have been counting in base-ten for almost two thousand years, if there was a problem, you'd think we'd have heard about it by now! ...so, obviously it works.

Here's the thing about modern mathematics - the *only* ideas we take as obvious are the axioms - those are the mathematical ideas that are so simple that they can't be expressed in yet other even-simpler ideas. The axioms are the minimal set of simple, obvious, irrefutable ideas from which everything else in mathematics is built[*].

As obvious as it seems, the fact that we can use base-ten to represent the integers is NOT among the list of axioms.

However because base-ten numbers are in a perfect one-to-one correspondence with the integers then it's safe to think of each integer's unique base-ten label *as* the integer. But to firmly establish this fact we need to (at least once) take the time to spell out exactly what it means to represent a number in base-ten with a theorem[†]. Then that theorem must be proven to be true with a series of arguments that logically connects it directly[‡] to the axioms, so that the only way that the theorem could be false is if the axioms themselves are false.

I could just state the "Base-Ten Representation Theorem" right here, but how to get to its clear, simple and succinct statement is an interesting journey. The rest of the paper is that journey. In fact we're going to end up generalizing upon our intuitive understanding about counting with base-ten and come up with a better theorem that covers base-ten and more. At the very least this new understanding will help you to "get" the cryptic joke about binary on page one!

---

[*]The axioms: For every integer a, b and c: Associativity: $(a + b) + c = a + (b + c)$ and $a(bc) = (ab)c$; Commutativity: $a + b = b + a$ and $ab = ba$; Distributive: $a(b + c) = (b + c)a = ab + ac$; Identities: There are integers 0 and 1 such that, $a + 0 = 0 + a = a$ and $a \cdot 1 = 1 \cdot a = a$ and Additive Inverse: $a + (-a) = 0$. Note: in general integers do NOT have multiplicative inverses that are also integers. (eg. $\frac{1}{2}$ is the multiplicative inverse of 2 because $\frac{1}{2} \cdot 2 = 1$ but $\frac{1}{2}$ is not an integer!)

[†]I can't find where the first such theorem was stated, I think it's quite recent.

[‡]directly ... or indirectly via other previously proven theorems.

We intuitively know that counting with base-ten covers all the positive integers. For example, the odometer in your car that keeps churning out new numbers for each mile you drive, starting from zero when it rolls off the production line. If your odometer was long enough that it stretched off past the horizon on your left, there's no limit on how many miles you could count.

Our intuition is good - let's write it down in our theorem. We might say:

Base-Ten Representation Theorem (initial draft)

Every integer has a representation in base-ten.

Something else we know intuitively is that each number written in base-ten represents only ONE integer. It almost feels silly to spell it out, but if we were to count out 4 piles of 100-apples-each-pile, then 9 piles of 10-apples-each-pile, then count out 9 additional apples, *then* scoop them all into a big pile that we'd always get the exact same size big-pile-of-apples.

It goes the other way too. If we were handed the aforementioned big-pile-of-apples we could start counting out piles of 100. We'd try to make as many piles of 100 as we could, and we'd find that we'd have 4 piles of 100 before we couldn't make another such pile. Then we would start counting out piles of 10 with the remaining apples. After we made as many piles of ten as we could out of those remaining apples, we would discover that we'd have 9 such piles of ten with 9 apples left over, in other words 499 apples! There is NO other way to divvy up this big-pile-of-apples if we follow this procedure. In other words, each integer is represented by only ONE base-ten number.

Let's strengthen our theorem based on the last two observations.

Base-Ten Representation Theorem (second draft)

Every integer has a *unique* representation in base-ten.

We can also restrict our theorem to positive integers, becauase we know that for every positive integer there exists a unique negative integer (such that if you add them together you get zero). So if we can prove the Base-Ten Representation Theorem for the positive integers then we can easily extend it to the negative integers (and zero) with a corollary. Our corollary could say something like "Slap a '-' (minus) sign in front of the positive base-ten representation to get a unique representation for it's negative counterpart" . . . or some such words.

Also, moving forward it would be helpful to have a name for our positive integer so that we can refer to it directly - how about n for "number":

Base-Ten Representation Theorem (third draft)

Every *positive* integer n has a unique representation in base-ten.

At the moment it's not very helpful to have named n (the theorem as it stands doesn't say anything more about n so why did we bother naming it?) but as we flush out the remaining details of the theorem we can refer to n which carries the important information that it could be ANY positive integer.

Earlier we looked at the number 92507 by adding up each digit times a power-of-ten[*]:

$$92507 = 9{\cdot}10^4 + 2{\cdot}10^3 + 5{\cdot}10^2 + 0{\cdot}10^1 + 7{\cdot}10^0$$

Every base-ten number implicitly describes an algebraic expression like this, so let's come up with a general expression of this form that can describe ANY positive integer n.

Let's replace one of the digits in our example number 92507 with d, how about the 5 like this 92d07. What I mean becomes clear if I write it out:

$$n = 92d07 = 9{\cdot}10^4 + 2{\cdot}10^3 + d{\cdot}10^2 + 0{\cdot}10^1 + 7{\cdot}10^0$$

So n is one of the following numbers: 92007, 92107, 92207, 92307, 92407, 92507, 92607, 92707, 92807 or 92907.

As you can see, the digit d must be an integer between 0 and 9 inclusive which we can write as "$0 \leq d \leq 9$" however I suggest that "$0 \leq d < 10$" is better[†]! It's logically equivalent to "$0 \leq d \leq 9$" but conveys more important information to the reader. Why even talk about nine when the theorem is about base TEN?

$$n = 9{\cdot}10^4 + 2{\cdot}10^3 + d{\cdot}10^2 + 0{\cdot}10^1 + 7{\cdot}10^0, \text{ where}$$
$$d \text{ is an integer such that } 0 \leq d < 10$$

This statement for n only represents the integers 92007, 92107, ... or 92907, so let's come up with a statement for n that will allow us to generate ANY five-digit number from 10000 the way up to 99999 (which is a complete list of all the five-digit numbers).

In order to describe this general five-digit number, we need five different 'd's, one for each of the five digits. In other words, we need to associate a different term d with each of the powers 10^4, 10^3, 10^2, 10^1 and 10^0.

Mathematics has a convention for coming up with a list of terms for situations just like this - we tack a subscript onto the name like so: d_2 which you read as "dee-two"[‡]. d_2 is a term to represent a digit just like the d we used above. But now we can use that little subscript as a way to associate it to a specific power-of-ten. Naturally we'll associate d_2 with 10^2 (ten squared) as follows:

$$n = 9{\cdot}10^4 + 2{\cdot}10^3 + d_2{\cdot}10^2 + 0{\cdot}10^1 + 7{\cdot}10^0, \text{ where}$$
$$d_2 \text{ is an integer such that } 0 \leq d_2 < 10$$

If we define d_2 like this, then we know that when we refer to the digit d_2 that we are talking about the digit that is multiplied with 10^2.

---

[*]It's time to replace our "$\times$" symbol for multiplication, with "$\cdot$" because "$\times$" might get confused for an "x" in an expression, whereas "$\cdot$" never will be. Eg. $x \times 2$ vs. $x \cdot 2$, additionally ending up with something that is more aesthetically pleasing. You may also see the "$\cdot$" omitted entirely as in ab - which means $a \cdot b$ as you have seen in earlier footnotes.

[†]Read $0 \leq d \leq 9$ as "zero is less-than-or-equal-to dee which is less-than-or-equal-to nine" and $0 \leq d < 10$ as "zero is less-than-or-equal-to dee which is (strictly) less-than ten".

[‡]...yes like artoo-detoo, which perhaps George should have writen as "$R_2 D_2$" and not "R2-D2"!

Let our five-digit-number n use d_0, d_1, d_2, d_3 and d_4 for its digits. Then the general expression for n looks like this[*]:

$$n = d_4 \cdot 10^4 + d_3 \cdot 10^3 + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0, \text{ where}$$

d_0 is an integer such that $0 \leq d_0 < 10$, and

d_1 is an integer such that $0 \leq d_1 < 10$, and

d_2 is an integer such that $0 \leq d_2 < 10$, and

d_3 is an integer such that $0 \leq d_3 < 10$, and

d_4 is an integer such that $1 \leq d_4 < 10$.

Ok, hold on a minute - that's getting a little cumbersome. it's clunky and hard to read - plus did you notice how we slipped in that different range for d_4?

First let's deal with the different range on that d_4. To make sure n is a legitimate five-digit number we have to call out the exception that d_4 can NOT be zero - it has to be at least 1. Why? Because if d_4 were zero then n would only be a four-digit number, or perhaps a three-digit number, or only two-digits etc.

Secondly, to clean up the presentation a common convention is to let another term like i, for perhaps "index", stand in for the subscript when you want to talk about all your 'd's at once:

Let d_0, d_1, d_2, d_3 and d_4 be integers such that:

$$n = d_4 \cdot 10^4 + d_3 \cdot 10^3 + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$$

where $0 \leq d_i < 10$ for all i in $\{0, 1, 2, 3, 4\}$ and $d_4 \neq 0$.

That's it! Those statements, and the expression for n describe EVERY five-digit number.

Now let's extend our five-digit expression for n to an arbitrary number of digits. Consider the following progression:

expression for n	number-of-digits
$d_0 \cdot 10^0$	1
$d_1 \cdot 10^1 + d_0 \cdot 10^0$	2
$d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$	3
$d_3 \cdot 10^3 + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$	4
$d_4 \cdot 10^4 + d_3 \cdot 10^3 + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$	5
$\ldots$	$\ldots$
$d_k \cdot 10^k + \ldots + d_4 \cdot 10^4 + d_3 \cdot 10^3 + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$	k+1

Using k like this let's us specify any number of digits we want. If we let $k = 0$ we get the first "single digit" item on the list. $k = 4$ gives us our five-digit number above, or we could let k be a billion, which would allow us to specifcy an integer that has a billion-and-one digits in it[†]!

---

[*]That expression looks like hard-core math, so let's take a moment to read it out loud, as a Math-Professor might do in a lecture. She might say: "n is equal to dee-four times ten-to-the-fourth, ... plus dee-three times ten-cubed, ... plus dee-two times ten-squared, ... plus dee-one times ten, ... plus dee-zero times one."

[†]A billion-and-one digit number is *ridiculously* large, consider that our estimate of the number of molecules in the entire universe would only need a base-ten number with the k set to somewhere between 78 and 82 to count them all.

So there we have it, we found our expression for being able to express each positive integer, let's use it in a revised draft of our theorem:

Base-Ten Representation Theorem (close to final draft)

For every positive integer n there is a unique sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$$n = d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$$

where $0 \leq d_i < 10$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \neq 0$.

Definition: n is represented in base-ten by the string of digits $d_k d_{k-1} \cdots d_2 d_1 d_0$

Our newly added "Definition" introduces exactly what it means to write the number out in base-ten; that is, we toss out all the extraneous stuff from our expression and string all the digits one after another. Starting at the most-significant digit d_k on the left, down to the next digit to its right which is d_{k-1} (read as "dee-kay-minus-one"[*]) all the way down to the least-significant units-digit d_0 on the right.

We are so darn close, but there is one super-picky detail that we should be concerned about. Our theorem establishes what it means to represent a number in base-ten, so until we've proven it, how can we actually use the first two-digit number "10" to represent the integer ten!? We need a symbol for ten in the theorem, so what can we do?

Apart from "10" we don't have a symbol for the integer ten so we have to make one up, how about T for "Ten":

Let T represent the integer ten.

For every positive integer n there is a unique sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$$n = d_k \cdot T^k + d_{k-1} \cdot T^{k-1} + \cdots + d_2 \cdot T^2 + d_1 \cdot T^1 + d_0 \cdot T^0$$
$\ldots$ etc.

That's a little confusing, so let's solve our problem by defining the two digit number "10" (i.e., a one followed by a zero) to be the integer ten. It's ok - we're not violating any rules by doing this. At this point we're just defining a symbol to stand in for the integer ten. Here's our FINAL draft of the theorem:

Base-Ten Representation Theorem

Let the two digit number "10" represent the integer ten.

For every positive integer n there is a unique sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$$n = d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$$

where $0 \leq d_i < 10$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \neq 0$.

Definition: n is represented in base-ten by the string of digits $d_k d_{k-1} \cdots d_2 d_1 d_0$

---

[*] $\ldots$ and d_{k-1} is multiplied by "ten-to-the-power-of-(kay-minus-one)".

Consider that base-ten is not the only base in use these days. Since the introduction of the EDVAC* computer, around 1950, there have been many orders of magnitude more calculations done in base-two (otherwise known as binary) by computers than have EVER been done by people in base-ten for the entirety of human history. (This might even be true if we only count one-day's worth of binary computer calculations - someone needs to check this.)

Binary-computer logic gates (the building blocks of the modern computer) can only take one of two states, that is; "off" or "on". We interpret these two states to represent these two numbers: 0 and 1. By doing so, in the same way that base-ten uses ten numbers 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9 for its digits; we can represent integers in base-two with just the digits 0 and 1. How is this possible? Let's find out with an imaginary trip into space.

Consider distant Planet-Nova on which the emergent intelligent species only have nine fingers on their hands. They have three hands with three fingers each - anyway, that's why they use base-nine, so they only need the numbers 0, 1, 2, 3, 4, 5, 6, 7 and 8 for their digits†. So like we Earthlings do for the integer ten, instead of making up a new symbol for nine, they use "10" to represent the integer nine - which for them means "One lot of nine, plus zero units".

Similarly on Planet-Ocho, since they only have eight fingers, then they use base-eight and only use numbers 0, 1, 2, 3, 4, 5, 6 and 7 for their digits. For them "10" means "One lot of eight, plus zero units".

On and on past Planet-Gary-Seven, and Planet-Secks, Planet-Penta, . . .

Finally we come upon Planet-Claire (well someone has to come from Planet-Claire, I know she came from there), where the poor blighters only have two fingers so they only use the digits 0 and 1 and base-two, so for them "10" means "one lot of two and zero units". So on Planet-Claire "10" means two. Recall above how we arrived at our 100 in base-ten, being "ten lots of ten, plus zero units" - similarly on Planet-Claire "100" in base-two for them means "Two lots of two plus zero units" in other words, four! What is "11" in base-two? Using our technique to describe the digits we see that it's "One lot of two, plus one unit", in other words three.

Here's how they count on Planet-Claire using base-two:

base-two	base-ten	base-two	base-ten
0	0	(. . . cont)	
1	1	1101	13
10	2	1110	14
11	3	1111	15
100	4	10000	16
101	5	10001	17
110	6	. . .	
111	7	11111	31
1000	8	100000	32
1001	9	. . .	
1010	10	1000000	64
1011	11	10000000	128
1100	12 (cont. . .)	100000000	256

---

*You might be thinking, don't you mean ENIAC which was earlier? Actually no - the ENIAC used base-ten accumulators, not binary!

†Digit is another word for finger! Of course that's where the math term got its start.

Note something interesting in the list above - the powers of two, written in base-two, resemble our powers of 10 in base-ten! That is:

$$1 = 2^0 = 1,$$
$$2 = 2^1 = 10_{\text{(base-2)}},$$
$$4 = 2^2 = 100_{\text{(base-2)}},$$
$$8 = 2^3 = 1000_{\text{(base-2)}},$$
$$16 = 2^4 = 10000_{\text{(base-2)}},$$

$$32 = 2^5 = 100000_{\text{(base-2)}},$$
$$64 = 2^6 = 1000000_{\text{(base-2)}},$$
$$128 = 2^7 = 10000000_{\text{(base-2)}},$$
$$256 = 2^8 = 100000000_{\text{(base-2)}},$$
$$\cdots$$

Let's look at the binary number 11010 for example. Using our wordy technique to describe the number we can see that it's "One lot of sixteen, plus one lot of eight, plus zero lots of four, plus one lot of two, plus zero units":

	1	×	10000			10000	(16)
+	1	×	1000		+	1000	(8)
+	0	×	100	=	+	000	
+	1	×	10		+	10	(2)
+	0	×	1		+	0	
					=	11010	(26)

Written in terms of powers of two: $11010_{\text{(base-2)}} = 26 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$.

Does that expression look familiar? It has exactly the same form as the expression for our five-digit base-ten number 92507. All the reasoning we used to come up with the statement of the "Base-Ten Representation Theorem" can be used again, but swapping powers-of-two for powers-of-ten, and limiting the values for the digits to be zero or one. Following our line of reasoning this is what the Planet-Claire mathematicians would have come up with:

Base-Two Representation Theorem

For every positive integer n there is a unique sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$$n = d_k 2^k + d_{k-1} 2^{k-1} + \cdots + d_2 2^2 + d_1 2^1 + d_0 2^0,$$

where $0 \leq d_i < 2$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \neq 0$.

Definition: n is represented in base-two by the string of binary-digits $(d_k d_{k-1} \cdots d_2 d_1 d_0)_2$

Our new Base-Two Representation Theorem introduced some helpful new notation. How do you know what I'm talking about if I just write "1000"? Do I mean 10^3 or 2^3? If there is any possibility for confusion we write the number like this $(1000)_{10}$ for the base-ten version meaning one-thousand and $(1000)_2$ for the binary version meaning eight. That's what the "Definition" is spelling out with the "$(\ldots)_2$" extra notation.

As is hinted by the habits of our various alien friends above it seems that we can use ANY integer greater than or equal to 2 as a base (base-one doesn't really make sense - think about it for a while). In fact computer graphics artists are known to stumble upon numbers written in hexadecimal (usually relating to specifying a color-channel), which is base-sixteen.

Base-sixteen introduces some new single-character symbols to the usual numbers 0, 1, 2, thru 9, to represent the numbers 10, 11, 12, 13, 14 and 15. Base-sixteen adds the digits A, B, C,

D, E and F where $A_{16}=(10)_{10}$, $B_{16}=(11)_{10}$, $C_{16}=(12)_{10}$, $D_{16}=(13)_{10}$, $E_{16}=(14)_{10}$, $F_{16}=(15)_{10}$. So $(80FB)_{16}$ is a four digit number in base-sixteen. (As we'll see shortly it means $(33019)_{10}$ in base-ten).

Note that if we omit the parentheses and subscript from a number, it means we're talking about it in base-ten; our "default" base. Case in point: the subscripts that we use to denote the base (like the "16" in $(80FB)_{16}$) are written in base-ten!

We could go ahead and prove our "Base-Ten" and "Base-Two" theorems above, but what about proving the "Base-Nine" version of the theorem for the aliens on Planet-Nova, or the "Base-Eight" version for the inhabitants of Planet-Ocho?

To cover all bases (pun intended) let's restate our theorem for the general case, call it "base-b", where b is some number greater than or equal to two. If we can prove that theorem, then we'll automatically get all the cases of specific bases for free.

Basis Representation Theorem

Let b be a positive integer greater than 1.

For every positive integer n there is a unique sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0,$$

where $0 \leq d_i < b$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \neq 0$.

Definition: n is represented in base-b by the string of base-b-digits $(d_k d_{k-1} \cdots d_2 d_1 d_0)_b$

So to get the "Base-Ten Representation Theorem" let b equal ten. To get the "Base-Two Representation Theorem" let $b = 2$; or the "Base-Nine Representation Theorem" let $b = 9$; etc.

The Basis Representation Theorem implies that we can safely convert between different bases. Why? (Exercise left for student).

Recall how we defined $(A)_{16} = 10$ and $(F)_{16} = 15$ as base-sixteen digits, then:

$$(97A3F2)_{16} = 9 \cdot 16^5 + 7 \cdot 16^4 + 10 \cdot 16^3 + 3 \cdot 16^2 + 15 \cdot 16^1 + 2 \cdot 16^0 = 9,937,906$$

... which gives you an idea of how you can convert from an alternate base into base-ten.

We should extend the Basis Representation Theorem to include all the integers.

We can take comfort in knowing that this shouldn't be too difficult. 0 itself is a perfectly acceptable representation for zero in all bases. Actually, we could have included zero as part of the original theorem if we had just allowed for the exception: "...and $d_k \neq 0$ except when $n = 0$", but at this point we're just talking about book-keeping type details.

Also, as we discussed earlier, since negative numbers are unique (they pair one-to-one with their positive counterpart) then by simply adding a new symbol like "-", and defining what "-1" means, we should be able to make an extension to the theorem that defines unique representations for negative numbers fairly easily.

Epilogue

At this point we really ought to get to the proof of the Basis Representation Theorem.

However truth be told, the proof supplied below, while elementary, isn't the most beautiful proof in the world and thus not necessarily the best to follow for the first time mathematician. In fact here's what one of the world's greatest mathematicians[*], G. H. Hardy, had to say about such proofs[†]:

> "We do not want many 'variations' in the proof of a mathematical theorem: 'enumeration of cases', indeed, is one of the duller forms of mathematical argument. A mathematical proof should resemble a simple and clear-cut constellation, not a scattered cluster in the Milky Way."

I couldn't agree more which is why I'm pushing the proof to a section at the end of this paper, which you may feel free to skip. I still invite you to to take a stab at following it, I tried my best to make it clear and interesting, but don't feel bad if it makes your head hurt. If you do try to follow it - it does have some points of interest - not the least of which is that it works but more importantly you'll learn about a very powerful tool called "The Principle of Mathematical Induction".

I think at this point you are well equipped you to try your hands at a couple of exercises for fun. If you get stuck, or to check your work, the answers are also supplied below - but please don't peek until you try the questions yourself!

Exercises

1. What are the following numbers expressed in base-ten?

    i) $(110101)_2$

    ii) $(A053D)_{16}$

    iii) $(1017)_{23}$

2. What are the following base-ten numbers expressed in an alternate base?

    i) 33 expressed in base-two?

    ii) 127 expressed in base-two? (Hint: $127 = (128 - 1)$)

    iii) 8079 expressed in base-sixteen?

    Hint: For a moment, pretend that we don't use base-ten to write out our numbers, instead picture a pile of apples. Can you picture 7654 apples? Yes? Good let's use 7654 as our example.

    Let's divide 7654 by 10 so we get the following:

    $$7654 = 765 \cdot 10 + 4$$

---

[*]along with the Gauss and Euclid mentioned later in this paper.
[†]in an essay he wrote called "A Mathematician's Apology".

Notice the remainder 4 is the least significant digit of our integer 7654 (i.e. the d_0 digit in the theorem).

How do we get the next digit, i.e. the d_1 digit that corresponds to the 10^1 term? Well, it's kind of cheating, but since we happen to be looking at that last expression written in base-ten we can see it sitting right there in at the end of the quotient "765". So, let's use the same technique and divide 765 by 10:

$$765 = 76 \cdot 10 + 5$$

So the remainder is 5 our d_1 digit. Let's keep going, this time dividing the previous quotient 76 by 10....

$$76 = 7 \cdot 10 + 6$$

and finally,

$$7 = 0 \cdot 10 + 7$$

So, our series of remainders happens to be the digits of the number in base-ten. Specifically $d_3 = 7$, $d_2 = 6$, $d_1 = 5$ and $d_0 = 4$.

Try doing that for 8079, but use 16 instead of 10 as the divisor.

iv) Let $A_{23} = 10, B_{23} = 11, C_{23} = 12, D_{23} = 13, E_{23} = 14, F_{23} = 15, G_{23} = 16,$
$H_{23} = 17, I_{23} = 18, J_{23} = 19, K_{23} = 20, L_{23} = 21$ and $M_{23} = 22,$
then what is 185190 expressed in base-twenty-three?

v) 291480 expressed in base-twenty-three?

Answers

1. What are the following numbers expressed in base-ten?

    i) $(110101)_2 = 53$

    ii) $(A053D)_{16} = 656701$

    iii) $(1017)_{23} = 12197$

2. What are the following base-ten numbers expressed in an alternate base?

    i) $33 = (100001)_2$

    ii) $127 = (1111111)_2$

    iii) $8079 = (1F8F)_{16}$

    iv) $185190 = (F51H)_{23}$

    v) $291480 = (10M01)_{23}$

The Principle of Mathematical Induction

As we discussed way up at the top of this paper, we think about generating the set of positive integers as a process that builds them up one by one. That is, each successive integer is one more than the previous one, starting at 1, then one more taking us to 2, then 3, 4, 5, ...ad infinitum[*].

This idea of being able to step one after the other, beginning at 1 and going forever is embodied within the principle of mathematical induction and is a basic property of the positive integers. This principle is more than just a way to generate the set of integers, it's also a way of thinking about properties of the integers.

Suppose that $P(n)$ means that the property P holds for the number n; where n is a positive integer. Then the principle of mathematical induction states that $P(n)$ is true for ALL positive integers n provided that[†]:

  i) $P(1)$ is true

 ii) Whenever $P(k)$ is true, $P(k + 1)$ is true.

Why would these two conditions show that $P(n)$ is true for all positive integers? Note that condition ii) only asserts the truth of $P(k+1)$ under the assumption that $P(k)$ is true. However if we also know that $P(1)$ is true then condition ii) implies that $P(2)$ is true, which again implies that $P(3)$ is true, which in turn leads to the truth of $P(4)$, etc., over and over for all positive integers.

Some people picture an infinite row of dominoes. Having condition i) (called the "base case") is like being able to knock over the first domino. Then knowing condition ii) is also true (called the "induction step") is like the fact that any one domino has the ability to knock over the next. Once you've knocked over the first domino, they all fall.

Let's look at a simple example: Perhaps you've heard the story of young Carl Friedrich Gauss as a boy in the 1780s who was assigned (along with all his classmates) the tedious task of summing the first 100 integers - presumably to keep them quiet and busy while the teacher corrected some papers. Anyway, young Gauss immediately produced the answer, 5050, before most of the boys had summed the first couple of numbers.

It wasn't young Gauss's extraordinary computational speed which allowed him to perform this dazzling task, but he had the deeper insight that instead of adding 1 plus 2, then adding 3, then 4, etc. he saw that if you paired 1 with 100, and 2 with 99, and 3 with 98, etc., that each of those pairs added up to 101, furthermore he knew he'd have 50 such pairs, meaning he could state the result in a heartbeat - tada - "5050"! Gauss is widely regarded as being one of the greatest mathematicians who has ever lived - the young eight-year old was just getting started.

---

[*] "ad infinitum" means "to infinity", or "continue forever, without limit".

[†] This wording of the definition of "The Principle of Mathematical Induction" is essentially borrowed from "Calculus" by Michael Spivak - a fabulous introductory textbook on Analysis.

Anyway, to generalize young Gauss's insight we can write the expression like this:

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

So let's prove this relationship using the principle of mathematical induction.

Let $n = 1$ for the "base case", then

$$\frac{1(1+1)}{2} = \frac{2}{2} = 1$$

Which is the trivial sum* of the first positive integer 1.

Now let's assume the relationship is true for n, and prove that it must also be true for $n+1$ for our "induction step":

$$(1 + 2 + 3 + \ldots + n) + (n+1)$$
$$= \frac{n(n+1)}{2} + (n+1)$$
$$= \frac{n(n+1)}{2} + \frac{2(n+1)}{2}$$
$$= \frac{n^2 + n + 2n + 2}{2}$$
$$= \frac{n^2 + 3n + 2}{2}$$
$$= \frac{(n+1)(n+2)}{2}$$
$$= \frac{(n+1)((n+1)+1)}{2}$$

Which proves young Gauss's expression is true for the positive integer $n+1$ whenever it's true for n - then by the principle of mathematical induction, the expression is true for all positive integers. QED[†]

Extra Exercise: Geometric Series Theorem

If b, n are nonnegative integers and $b \neq 1$ then prove,

$$1 + b + b^2 + \cdots + b^{n-1} = \frac{b^n - 1}{b - 1}$$

Hint: use induction on n, the base case being $n = 1$. Try it, you can do it!

---

*The word "sum" here is used in the context of the expression we are trying to prove. In this case we are summing only one item thus it's "trivial".

[†]"QED" - is often used at the conclusion of a proof to state that it's done - it's an acronym for the Latin phrase "quod erat demonstrandum" which means "that which was to be demonstrated". In other words we've proven what we set out to prove.

Proof for Extra Exercise: Geometric Series Theorem

Base case: $n = 1$

$$\frac{b^1 - 1}{b - 1} = \frac{b - 1}{b - 1} = 1 = b^0 = b^{1-1}$$

Induction step: Assume the following

$$1 + b + b^2 + \cdots + b^{n-1} = \frac{b^n - 1}{b - 1}$$

Then,

$$(1 + b + b^2 + \cdots + b^{n-1}) + b^n$$
$$= \frac{b^n - 1}{b - 1} + b^n$$
$$= \frac{b^n - 1}{b - 1} + \frac{b^n(b - 1)}{b - 1}$$
$$= \frac{b^n - 1 + b^{n+1} - b^n}{b - 1}$$
$$= \frac{b^{n+1} + b^n - b^n - 1}{b - 1}$$
$$= \frac{b^{n+1} - 1}{b - 1}$$

QED

Proof of the Basis Representation Theorem

How do we prove our theorem? There are several ways to approach it.

The mathematician George E. Andrews (in his book "Number Theory") has an interesting proof. He asks us to imagine a function that given a positive integer n, counts the number of base-b representations of n. Then with some fairly straightforward reasoning he shows that this counting-function MUST produce a count of "1" for every n, both establishing the uniqueness and the existence in one fell swoop. It's a cool proof - short and sweet, I'll bet G. H. Hardy would approve of it from an aesthetic standpoint.

We could also use the Euclidean Division Theorem to prove our theorem. We could show that by dividing our integer n by b, then dividing that result by b again, then again, and again, etc. that we'd get a series of remainders which are the base-b-digits of n. This is an interesting approach to the proof in that it also gives us a technique to construct a base-b representation of each integer. If we were to go down this road we would try to generalize how we solved exercise number 2-iii) above, it's worth a try for fun.

However, we're going to follow a much more straightforward approach. We'll use the principle of mathematical induction directly on n to prove that a base-b representation of each positive integer exists. Then we'll use a different approach to prove that each such representation is unique.

Using the principle of mathematical induction to prove that a base-b number exists for all the positive integers is pretty simple. The crux of the approach is to show that if n can be expressed in base-b, then it necessarily follows that $n + 1$ can also be represented in base-b.

This is best thought of as a magic odometer in your new magic car. As you pull it out of the dealership parking lot on the first day you notice its odometer is only one digit wide. That one and only display-digit shows a "1", I guess the factory was only one mile away.

As you get close to the end of your drive home you see you've clocked 9 miles. Naturally you're a little curious about how it's going to count to 10 since the odometer apparently only has one digit for counting. While pondering this curiosity you see the 9 starting to roll over back to 0, and a second digit to it's left magically materializes! It rolls to a 1 as the 9 settles back to 0. Nice new feature - the unlimited odometer! Apparently this magic odometer only adds new digits to the left as it needs them. The magic odometer should be able to display ANY number of miles, no matter how large. (Good thing too, this new line of magic cars from Tesla are guaranteed to last forever.)

Our proof is going to take care of the three cases that happen with the magic-odometer. Imagine that we've already driven some arbitrarily large number of miles, and we're watching the odometer roll over to the next mile. We have the following cases:

i) The units digit is less than 9, so driving one more mile only increments the units digit, not affecting any of the other digits.

Example: We've driven 782995 miles so far, so the next mile driven is $782995 + 1 = 782996$.

So that units digit turned from a "5" to a "6", all the rest of the digits remaining unchanged, so the new number is a legitimate base-ten number.

ii) The units digit, and perhaps a few directly to the left of it, are all 9's, so driving one more mile will spin all those 9's to 0, at the same time incrementing the rightmost digit *that isn't a* 9 by one.

Example: We've driven 782999 miles so far, so the next mile driven is:

$$
\begin{aligned}
782999 + 1 &= 780000 + 2999 + 1 \\
&= 780000 + (3000 - 1) + 1 \\
&= 780000 + 3000 + (-1 + 1) \\
&= 780000 + 3000 + 0 \\
&= 783000
\end{aligned}
$$

That looks overly complicated, but I broke it down like that to demonstrate the idea behind the algebraic "trick" that's used in the proof.

Anyway, it's clear that the rightmost digit that-isn't-a-9, in our case the 2, got changed to a 3 and all the 9's got changed to 0's, while the rest of the digits remained unchanged leaving us with a legitimate base-ten number.

iii) ALL the digits from the units digit up to the highest digit are 9's, so driving one more mile engages the magic odometer feature, materializing a new leftmost digit. The newly materialized digit turns to a 1 and all the 9's spin back to 0. In this case the number of digits on the odometer will have been extended by one.

Example: We've driven 999999 miles so far, so the next mile driven is:

$$999999 + 1 = (1000000 - 1) + 1$$
$$= 1000000 + (-1 + 1)$$
$$= 1000000 + 0$$
$$= 1000000$$

Same "trick" as the previous case, but this time our number grew from a six digit number to a seven digit number. Ya, we just drove a million miles which is definitely a legitimate base-ten number!

Even though we can use induction to prove the existence of base-b numbers for every integer, let's think about why it doesn't prove the "uniqueness" aspect of the theorem. Imagine a magic-box that also makes base-b representations for each integer. In other words, if the odometer is the P. of M. Induction then the magic-box is some different mechanism working in a different way. Why not? We weren't careful to show that induction is the ONLY way to generate a base-b representation for each number. (It isn't.)

So we need to prove that if such a magic-box exists then it MUST produce the same results as our odometer.

The easiest way to prove this, is to assume that there is a magic-box that DOES NOT produce the same representation as our odometer, then we show that this assumption leads to an irreconcilable contradiction. So either our assumption is wrong or the axioms are. Since we're VERY confident in the axioms being correct we can only conclude that our assumption must be wrong - meaning that there is only *one* way to make a base-b representation for each integer.

Without further adieu, let's get to the actual proof!

Existence Proof of the Basis Representation Theorem

Let b be a positive integer greater than 1.

We will show that for every positive integer n there is a sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0,$$

where $0 \leq d_i < b$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \neq 0$.

We will refer to the previous expression as the "base-b-representation" for n in the following induction proof.

Base case:

Consider when $n = 1$.

Let $d_0 = 1$ be the only integer in the sequence. Then,

$$d_0 b^0 = 1 \cdot b^0 = 1 \cdot 1 = 1 = n$$

Since $d_0 < b$ for all b and $d_0 \neq 0$ (note: $k = 0$) proving that a base-b-representation exists for the integer 1.

Induction Step:

Let n be a positive integer, and assume that there is a sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0,$$

where $0 \leq d_i < b$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \neq 0$.

We will prove that $n + 1$ also has a base-b-representation by looking at two cases.

Case 1) $d_0 < (b - 1)$

This case examines when the least significant digit of n is *strictly-less-than* the largest value it can take in base-b. (For example, in base-two $d_0 = 0$; In base-five $d_0 \leq 3$; In base-ten $d_0 \leq 8$.)*

$$
\begin{aligned}
n &= d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0 && \text{(Induction Assumption)} \\
\Leftrightarrow \quad n + 1 &= d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0 + 1 && \text{(Add 1 to both sides)} \\
&= d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0 + b^0 && \text{(Restate 1 as b^0)} \\
&= d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + (d_0 + 1) b^0 && \text{(Axiom of Distribution)}
\end{aligned}
$$

The expression for $n + 1$ uses the same sequence of integers $d_k, d_{k-1}, \ldots, d_2, d_1$ as n, with only change being that the integer d_0 was altered to $(d_0 + 1)$, but since:

$$
\begin{aligned}
d_0 &< (b - 1) && \text{(Case 1 Assumption)} \\
\Leftrightarrow \quad d_0 + 1 &< (b - 1) + 1 && \text{(Add 1 to both sides)} \\
\Leftrightarrow \quad d_0 + 1 &< b
\end{aligned}
$$

---

*Please read the following bidirectional arrow symbol $\Leftrightarrow$ as "if and only if" - it's like a logical "equals" sign

19

Therefore, given the conditions of "Case 1", $n+1$ has a base-b-representation whenever n does.

Case 2) $d_0 = (b-1)$

Now we'll look at the case when the least significant digit of n is *exactly-equal-to* the largest value it can take in base-b. (For example in base-two $d_0 = 1$; in base-five $d_0 = 4$; in base-ten $d_0 = 9$.)

We're going to split this case into two cases.

a) *All* the digits of n are equal-to $b-1$ (eg. 999999 in base-ten).

b) $d_0 = (b-1)$ but *at least one other* digit is not-equal-to $(b-1)$ (eg. 782999 in base-ten).

Then we're going to find out what happens when we add 1 to each case, thus giving us our resultant expression for $n+1$

Case 2a) ALL of the digits of n are equal to $(b-1)$.

So n can be expressed like this:

$$n = (b-1)b^k + \ldots + (b-1)b^2 + (b-1)b^1 + (b-1)b^0 \quad \text{(Induction Assumption)}$$

Recall in the "Extra Exercise: Geometric Series Theorem" we showed that:

$$1 + b + b^2 + \ldots + b^k = \frac{b^{k+1} - 1}{b - 1}$$

We can use this theorem to show that $n + 1 = b^{k+1}$ as follows:

$$b^k + \ldots + b^2 + b + 1 = \frac{b^{k+1} - 1}{b - 1} \quad \text{(Reorder terms of G.S.Thm.)}$$

$$\Leftrightarrow \qquad b^k + \ldots + b^2 + b^1 + b^0 = \frac{b^{k+1} - 1}{b - 1} \quad \text{(Rewrite with } b^1, b^0)$$

$$\Leftrightarrow \quad (b-1)(b^k + \ldots + b^2 + b^1 + b^0) = b^{k+1} - 1 \quad \text{(Mult both side by } (b-1))$$

$$\Leftrightarrow \quad (b-1)b^k + \ldots + (b-1)b^1 + (b-1)b^0 = b^{k+1} - 1 \quad \text{(Distribution of } (b-1))$$

$$\Leftrightarrow \qquad\qquad n = b^{k+1} - 1 \quad \text{(Substitute } n \text{ for expression)}$$

$$\Leftrightarrow \qquad\qquad n + 1 = b^{k+1} \quad \text{(Add 1 to both sides)}$$

We can rewrite $n+1$ as follows:

$$n + 1 = 1 \cdot b^{k+1} + 0 \cdot b^k + \ldots + 0 \cdot b^2 + 0 \cdot b^1 + 0 \cdot b^0,$$

Therefore, given the conditions of "case 2a", $n+1$ has a valid base-b-representation whenever n does. We note that the number of integers in the sequence associated with $n+1$ is one longer than for n. i.e., $n+1$ is one digit longer that n.

Case 2b) $d_0 = (b-1)$ but at least one other digit is not equal to $(b-1)$

Let j be the lowest power-of-b such that $d_j < (b-1)$, i.e.; we can write n as follows:

$$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_j b^j + (b-1)b^{j-1} + \cdots + (b-1)b^1 + (b-1)b^0$$

Similar to how we used the "Geometric Series Theorem" above, we can simplify the expression for n as follows:

$$n = d_k b^k + \cdots + d_j b^j + \left((b-1)b^{j-1} + \cdots + (b-1)b^1 + (b-1)b^0\right)$$
$$\Leftrightarrow \quad n = d_k b^k + \cdots + d_j b^j + (b^j - 1) \qquad \text{(Geom. Series Thm.)}$$
$$\Leftrightarrow \quad n + 1 = d_k b^k + \cdots + d_j b^j + b^j \qquad \text{(Add 1 to both sides)}$$
$$\Leftrightarrow \quad n + 1 = d_k b^k + \cdots + (d_j + 1)b^j \qquad \text{(Distr Axiom)}$$

Rewriting the expression for n in explicit terms:

$$n + 1 = d_k b^k + \cdots + d_{j+1} b^{j+1} + (d_j + 1)b^j + 0{\cdot}b^{j-1} + \ldots + 0{\cdot}b^1 + 0{\cdot}b^0$$

We can see that the expression for $n + 1$ uses the same sequence of integers $d_k, \ldots, d_{j+1}$ as n. The integer d_j was altered to $(d_j + 1)$, but since:

$$d_j < (b - 1) \qquad \text{(Previous assumption)}$$
$$\Leftrightarrow \quad d_j + 1 < (b - 1) + 1 \quad \text{(Add 1 to both sides)}$$
$$\Leftrightarrow \quad d_j + 1 < b$$

Furthermore the remaining sequence of integers $d_{j-1} = \ldots = d_2 = d_1 = d_0 = 0$.

Therefore, given the conditions of "case 2b", $n+1$ has a valid base-b-representation whenever n does.

Taking "Case 1" and "Case 2" together proves that $n+1$ always has a base-b-representation whenever n does. Having also established the base-case, therefore by the principle of mathematical induction all positive integers have a base-b-representation.

QED

In order to proceed with proving the uniqueness aspect of the Basis Representation Theorem, we need to make use of a well established theorem called the "Euclidean Division Theorem". It sounds onerous, but don't worry, you learned it in the third grade but perhaps not so formally, you called it "long division". It simply states the following:

Euclidean Division Theorem

For all integers a and b such that $b > 0$, there exist *unique* integers q and r such that[*]:

$$a = qb + r \text{ such that } 0 \le r < b$$

Definition: In the above equation:

    a is the *dividend*   ("the number being divided")
    b is the *divisor*   ("the number doing the dividing")
    q is the *quotient*   ("the result of the division")
    r is the *remainder*   ("the leftover")

This is how you first learned to divide. For example if someone asks you "What is nineteen divided by three?", you'd answer "six with one remaining". Here 19 is the *dividend*, 3 is the *divisor*, 6 is the *quotient* and 1 is the *remainder*. Written in the form of the theorem:

$$19 = 6 \cdot 3 + 1$$

Often proofs make use of little mini-theorems of their own. Creating these mini-theorems is a way to simplify a step in the main proof by establishing a useful intermediary result. It makes reading the main proof easier to follow by not having us get sidetracked with the technicalities of a step we want to make. These mini-theorems are called "Lemmas". We're going to make a lemma to help with proving the uniqueness part of the Basis Representation Theorem. But first we're going to make use of the Euclidean Division Theorem to prove our lemma.

Lemma

Let b, q and r be integers such that $b > 0$ and $0 \le r < b$, then:

$$0 = qb + r \qquad \text{if and only if} \qquad q = 0 \text{ and } r = 0.$$

Proof of Lemma

Let b, q and r be integers such that $b > 0$ and $0 \le r < b$, then

If $q = 0$ and $r = 0$, then
    $qb + r = 0 \cdot b + 0 = 0$

... and if $0 = qb + r$ then
    because the Euclidean Division Theorem says that q and r are unique, therefore
    $q = 0$ and $r = 0$ must be true otherwise they would not be unique.

QED

---

[*]Aside: Actually the theorem is stronger than we have stated here. Specifically, it only requires that $b \ne 0$, however to keep the remainder positive, the restriction on r would have to be stated like this $0 \le r < |b|$ to deal with the possibility that b might be negative.

Uniqueness Proof of the Basis Representation Theorem

Let b be a positive integer greater than 1.

By the "Existence Proof of the Basis Representation Theorem" we know that for every positive integer n there is a sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0$, where
$0 \leq d_i < b$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \neq 0$.

Assume this expression for n is not unique and that there also exists a different sequence of integers $c_0, c_1, c_2, \ldots, c_k$ such that:

$n = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_2 b^2 + c_1 b^1 + c_0 b^0$, where
where $0 \leq c_i < b$ for all i in $\{0, 1, 2, \ldots, k\}$ and $c_k \neq 0$.

Let's further suppose that j is the lowest power such that the integers $d_j \neq c_j$ and without any loss of generality let's assume that $d_j > c_j$. Since both expressions are equal to n then:

$$c_k b^k + \cdots + c_2 b^2 + c_1 b^1 + c_0 b^0 = d_k b^k + \cdots + d_2 b^2 + d_1 b^1 + d_0 b,$$

$$\text{if and only if,}$$

$$0 = (d_k - c_k) b^k + \cdots + (d_j - c_j) b^j \qquad \text{(Subtract LHS from both sides)}$$

$$\Leftrightarrow \quad \frac{0}{b^j} = \frac{(d_k - c_k) b^k + \cdots + (d_j - c_j) b^j}{b^j} \qquad \text{(Divide by } b^j, \text{ since } b > 0)$$

$$\Leftrightarrow \quad 0 = (d_k - c_k) b^{k-j} + \cdots + (d_{j+1} - c_{j+1}) b + (d_j - c_j) \qquad \text{(Divide each term in numerator by } b^j)$$

$$\Leftrightarrow \quad 0 = \big((d_k - c_k) b^{k-j-1} + \cdots + (d_{j+1} - c_{j+1})\big) b + (d_j - c_j) \quad \text{(Factor out common } b)$$

Let $q = \big((d_k - c_k) b^{k-j-1} + \cdots + (d_{j+1} - c_{j+1})\big)$, then

$$0 = qb + (d_j - c_j)$$

Since $0 \leq (d_j - c_j) < b$ and $b > 0$ then by our lemma we know that $q = 0$ and $d_j - c_j = 0$.

But $d_j - c_j = 0$ if and only if $d_j = c_j$ contradicting our assumption that $d_j \neq c_j$. This implies that the initial assumption that "n is not unique" is *false*, in other words:

$$\text{The base-}b \text{ representation of } n \text{ is unique.}$$
$$\text{QED}$$

Since we have proven that a base-b-representation exists for ALL the postive integers, *and* that this representation is unique, then we have proven the Basis Representation Theorem.